European Commission

AAA for INSPIRE Data and Services: Supporting access to geospatial data across Europe

NIST Federated Could Webinar, 29 October 2014

Robin S. Smith, Michael Lutz & Andreas Matheus

www.jrc.ec.europa.eu

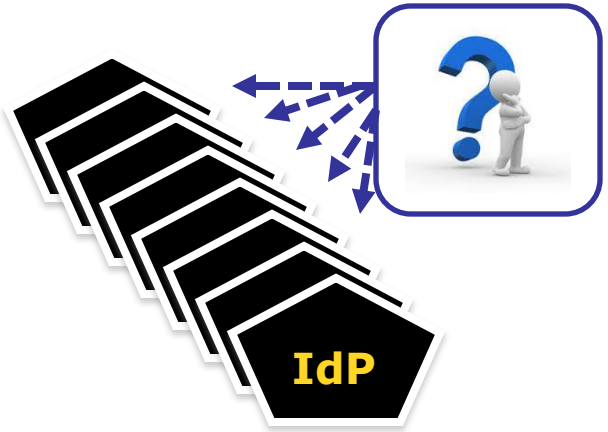
Serving society
Stimulating innovation
Supporting legislation

Joint Research Centre

ARe³NA
A Reusable INSPIRE Reference Platform

Overview

- ARE3NA in INSPIRE
- The AAA Approach
- SSO & IdP Discovery
- Lessons learned



- Thanks to the consortium!

geosparc
the geospatial architects

Secure Dimensions

KU LEUVEN

IDGIS

Joint Research Centre

ARe³NA
A Reusable INSPIRE Reference Platform

ARE3NA in INSPIRE

INSPIRE Directive 2007/2/EC*

VGI

Cross-sector apps

RDF & PID

Appl. Layer

Application and Geoportals

Internet

AAA

Service Layer

GeoRM Layers

Registry

Discovery Service

View Service

Download Service

Transf. Service

Harmonized SDS

Interoperable SDS

Invokable SDS

SDS

Network Services

SOS

harmonized

interoperable

invokable

discoverable

Data Layer

Registers

Service Metadata

Data Set Metadata

Spatial Data Set

Picrit

Re3gistry +

Metadata

*: Establishing an Infrastructure for Spatial Information in the European Community

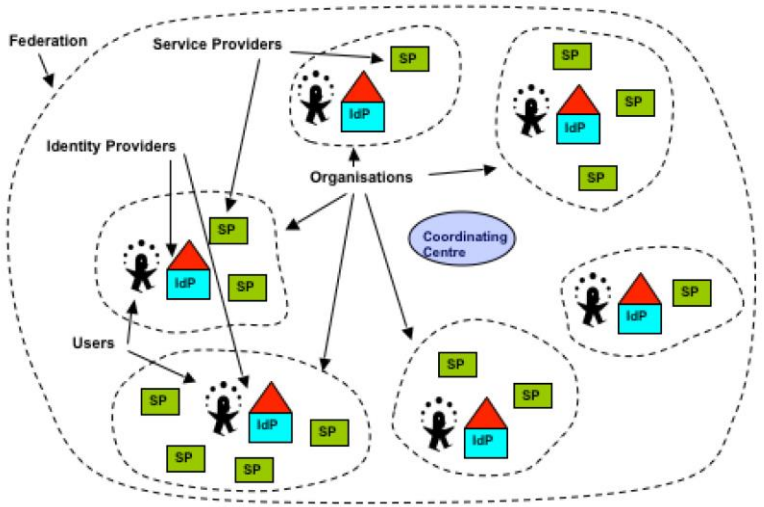
Validation

Background

- Access control in INSPIRE as a real technical experience.
  - Identify and assess current standards and technologies for secure data exchange, focussing on INSPIRE data and services.
  - Identify best practices of standards and technologies and identify what may be missing/reusable
- Involve stakeholders (workshop), develop a testbed (using open source tools to maximise reuse) and collect feedback on experiences.
- Technical activity for interoperability but organisational & social issues are emerging

AAA approach:
(Geo) Access Management Federation (AMF)

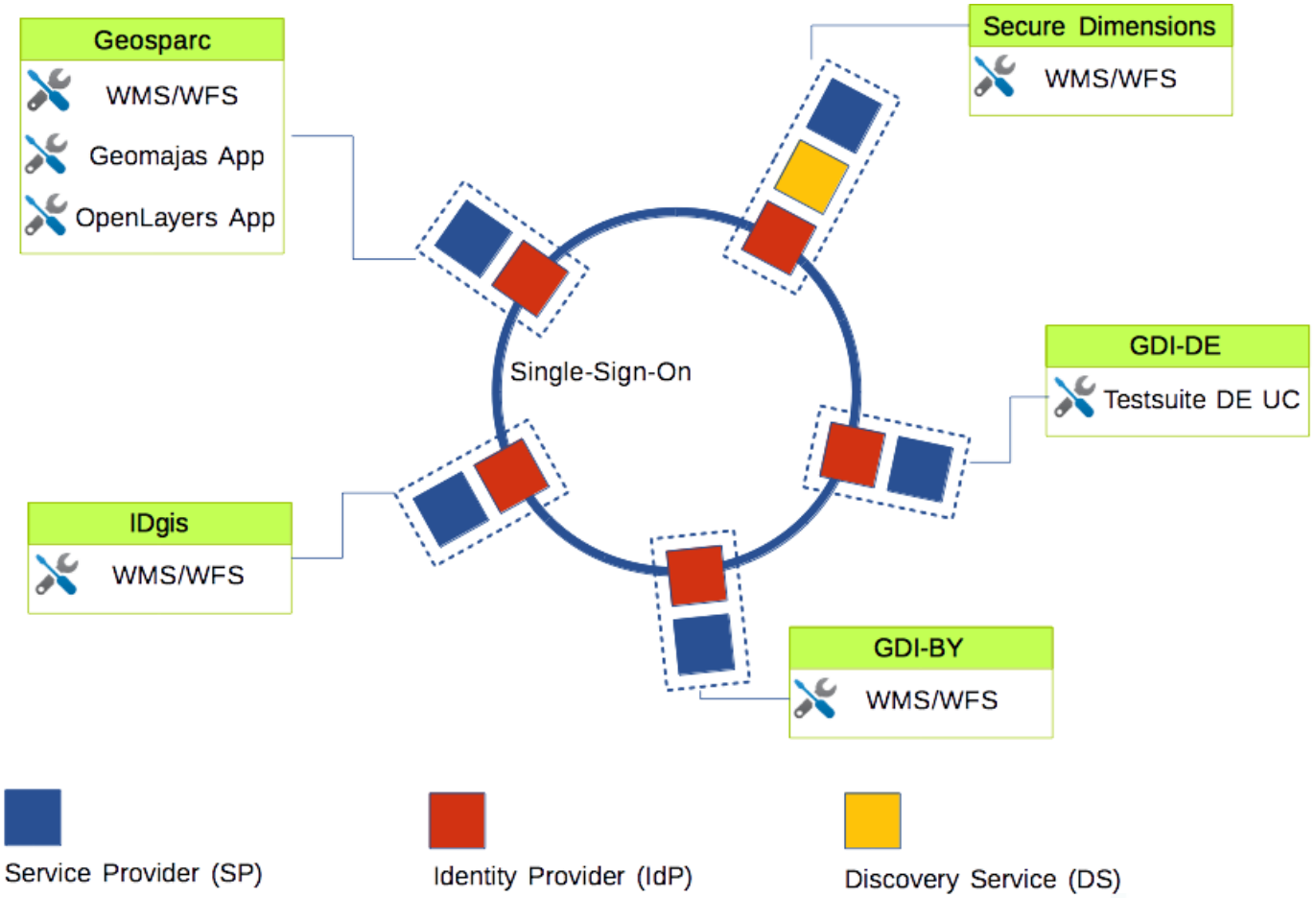
- Leveraging the concept of an ‘’Access Management Federation” from the Academia
  - In production around the world with 100m of users
  - https://www.aai.dfn.de/links/
- Authentication
  - Login via distributed IdPs
  - Authentication and Attribute Assertions with SAML
- Authorization
  - Local at each SP
  - XACML or GeoXACML policies
- Accountability
  - Local logging at each SP



ARe³NA
A Reusable INSPIRE Reference Platform

Joint Research Centre

AAA Testbed


Geosparc
WMS/WFS
Geomajas App
OpenLayers App
Secure Dimensions
WMS/WFS
Single-Sign-On
GDI-DE
Testsuite DE UC
IDgis
WMS/WFS
GDI-BY
WMS/WFS
Service Provider (SP)
Identity Provider (IdP)
Discovery Service (DS)

AAA – Use Cases (incomplete list)

- Use of protected View Services combined in one web-mapping application (e.g. OpenLayers)
  - Implications on Single.Sign.On, IdP Discovery and use of certain SAML profiles and bindings
- Use of protected View Services combined in a desktop GIS (e.g. QGIS)
  - Implications on Single.Sign.On and use of SAML profile
- INSPIRE compliance testing of service in Germany
  - Use the "Testsuite" hosted at SDI coordination office in Germany to enable compliance testing
  - Access policy (at each SP) ensuring access
    - Owner can access services unlimited
    - INSPIRE compliance testing "officer" has defined access
    - Any other user has no access to service(s)

Important differences to Academic AMF

Requirement	Academic AMF	AAA AMF or GeoAMF
IdP Discovery	User may choose multiple IdPs	User may only choose one single IdP
Single-Sign-On	New session establishment may involve user (IdP selection and attribute release acceptance)	New session establishment must work without user involvement and via Javascript libraries
SAML Profile / Binding	SAML Web Browser SSO Profile with POST Binding	SAML Web Browser SSO Profile with Artefact Binding
		SAML Enhanced Client Proxy Profile with PAOS Binding

Single-Sign-On and IdP Discovery

- Automatic session initiation requires to maintain user's decision of previously selected IdP (can only be one)
  - Leveraging of the SAML Identity Provider Discovery Profile and the Common Domain Cookie Writing Service
- AAA Testbed solution
  - Central IdP Discovery Service that acts as Common Domain Cookie Writing Service and IdP selection by user
- For ease of use
  - IdP Discovery Service supports persistent storage of IdP selection => User must select IdP only once
  - IdP Discovery Service supports "type and search"

Organizational Challenges: User Attributes and Access Rights

- Authorization is local at the SP based on user attributes
- Challenge: Service Provide is relying on
  - (i) IdP to submit mandatory attributes,
  - (ii) trust the value of the attributes
- Overall access rights management involves the federation wide agreement on user attributes (keys and possible values)
- Multi-Level-Policies to support enforcement of rights inherited from superseding policies
  - INSPIRE coordination (JRC) -> Member State -> Service Provider -> Resource(s)

Lessons Learned - Technical

- The SAML standard is complex and should not be implemented; deploy software frameworks such as Shibboleth to enable SAML based federation
- Deployment and configuration of Shibboleth rather straight forward; binary package available for almost all Operating Systems
- Deployment of Authorization layer is simple but declaration of XACML or GeoXACML policies is complex task as use case specific and user attributes dependent
- Browser security introduces additional challenges for web-mapping applications: CORS

Lessons Learned - Organizational

- Operation of a coordination centre is required
  - Maintain the federation metadata
  - Accept applications to join the federation, service level agreement validation, etc.
- Which user attributes do I need to enforce access rights for all the possible use cases
  - Mandatory user attribute definition with code lists
- What is the right level of granularity to enforce access rights on geospatial data services
- Proper indication of access constraints for a service within the ISO metadata
  - Authentication code list must be agreed and maintained

Conclusions

- Leveraging a proven concept from the Academia => Ensures scalability in terms of number of IdPs and SPs for a federation
- Separation of Authentication, Authorization and Accounting Layer
- Flexible in terms of access rights management => support for Mandatory and Discretionary Access Rights Management to ensure re-use of protected resources outside of INSPIRE
- Support of combined use of protected resources, in particular Web Services for geographic data, in web-mapping or desktop applications

Thank you

For more information
http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-17action_en.htm

robin.smith@jrc.ec.europa.eu
michael.lutz@jrc.ec.europa.eu
andreas.matheus@secure-dimensions.de

With thanks to the ARE3NA AAA Study consortium, especially Ann Crabbé, Danny Vandenbroucke, Andreas Matheus, Dirk Frigne, Frank Maes and Reijer Copier

ARe³NA

ARe³NA
A Reusable INSPIRE Reference Platform

Joint Research Centre